WHAT IS CLAIMED IS:

1. A method comprising:

fabricating a first plurality of FPGA integrated circuits with a first secret key embedded by way of a first mask set; and

fabricating a second plurality of FPGA integrated circuits with a second secret key embedded by way of a second mask set.

2. The method of claim 1 wherein a first secure bitstream will configure properly user-configurable logic of the first plurality of FPGA integrated circuits, but not the second plurality of FPGA integrated circuits.

3. The method of claim 1 further comprising:

loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream using the first secret key.

4. The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of FPGA integrated circuits with the second secret key are assigned to a second geographic area.

5. The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are fabricated in a first time period and the second plurality of FPGA integrated circuits with the second secret key are fabricated in a second time period, different from the first time period.

6. The method of claim 1 wherein only one mask differs between the first and second mask sets.

7. The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned exclusively to a first customer.

8. The method of claim 5 wherein the first time period is about the same duration as the second time period.

9. The method of claim 5 wherein the first time period is a different duration from the second time period.

10. The method of claim 6 wherein the one mask is a contact mask.

11. The method of claim 1 wherein there are random differences between artwork of the first and second plurality of FPGA integrated circuits in addition to the different embedded secret keys.

12. The method of claim 1 wherein the first and second secret keys are presented on wires of respective plurality of FPGA integrated circuits for only a limited duration.

13. The method of claim 1 wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory of the FPGA integrated circuit.

14. The method of claim 1 wherein the first secret key is embedded by changes to a relatively large block of logic in the first plurality of FPGA integrated circuits and its value extracted using a CRC algorithm.

15. The method of claim 13 further comprising:

extracting the first secret key by using a CRC algorithm to compute a checksum of the initial state of the device configuration memory.

16. The method of claim 1 further comprising:

loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number.

17. The method of claim 1 further comprising:

loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number, wherein the secure bitstream includes a message authentication code.

18. A method comprising:

embedding a first secret key within the artwork of an FPGA integrated circuit;

storing a user-defined second secret key within an encrypted FPGA bitstream stored in an external nonvolatile memory accessible by the FPGA;

decrypting the user-defined second secret key using the first secret key; and

setting up a secure network link between the FPGA and a server using the user-defined second secret key.

19. The method of claim 18 further comprising:

downloading an FPGA bitstream using the secure network link;

encrypting the downloaded FPGA bitstream using the first secret key; and

storing the encrypted downloaded bitstream in the external memory.

20. The method of claim 18 wherein the secure network link is created using a standard internet security protocol.

21. The method of claim 18 further comprising:

configuring the FPGA using the encrypted downloaded bitstream stored in the external memory.

22. A method comprising:

storing a first secret key on an FPGA chip;

causing the FPGA to calculate a message authentication code (MAC) corresponding to a user design; and

storing the message authentication code with bitstream information in a nonvolatile memory.

23. The method of claim 22 further comprising:

storing copyright messages with the bitstream information;

detecting unauthorized alterations to the bitstream using the message authentication code; and

preventing bitstreams which have been altered from being used to configure an FPGA.

24. The method of claim 22 further comprising:

recording the message authentication code along with corresponding identification information for a product containing the FPGA; and examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification.

Add a1